161. ***3.*** *Державний стандарт України. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. ДСТУ 4145. Київ, Держстандарт України, 2003.* ***4.*** *Itoh T., Tsijii S. A Fast Algorithm for Computing Multiplicative Inverses in* $GF(2^m)$ *Using Normal Bases. // Info. and Comput., 78(3), 1988, 171–177.* ***5.*** *Koblitz N. Elliptic Curve Cryptosystems // Mathematics of Computation, 48, 1987, 203 – 209.* ***6.*** *Miller V. S. Use of Elliptic Curves in Cryptograph y // Advances in Cryptology – Crypto'85 (LNCS 218), 1986, 417 – 426.* ***7.*** *Silverman J. The Arithmetic of Elliptic Curves. – New York: Springer, 1986.* ***8.*** *Silverman J. Advanced Topics in the Arithmetic of Elliptic Curves. – New York: Springer, 1994.* ***9.*** *Menezes A. Elliptic Curve Public Key Cryptosystems. – Boston: Kluwer Academic Publishers, 1993.* ***10.*** *Blake I., Seroussi G., Smart N. Elliptic Curves in Cryptography. – Cambridge University Press, 1999.* ***11.*** *Cohen H., Miyaji A., Ono T. Efficient Elliptic Curves Exponentiation Using Mixed Coordinates // Advances in Cryptology –Asiacrypt'98 (LNCS 1514), 1998, 51–65.*

УДК 691.3.06

МЕТОД ГЕНЕРУВАННЯ ПАРАМЕТРІВ ЕЛІПТИЧНИХ КРИВИХ

Микола Карпінський*, Ігор Васильцов, Ігор Якименко, Ярослав Кінах

**Університет в Бєльську-Бялей, Польща,*

Тернопільська академія народного господарства.

Анотація: **Розглядається проблематика генерування параметрів еліптичної кривої. Розроблено метод, що дозволяє ефективно визначати коефіцієнти еліптичної кривої. Розроблений метод базується на застосуванні еволютивного підходу. В статті наведено результати роботи програми, розробленої на основі даного методу.**

Summary: **In this paper the problem of generating of elliptic curves parameters has been considered. To obtain the coefficients of elliptic curve the method has been developed. This method is based on the usage of evolutionary approach. In the paper the results of software, developed on the proposed method, have been shown.**

Ключові слова: **Еліптична крива, еволютивний алгоритм, цифровий підпис.**

І Застосування еліптичних кривих для задач захисту інформації

Захист інформації відіграє одну з ключових ролей в забезпеченні інформаційної безпеки держави. В останні роки в зв'язку з швидким розвитком інформаційних технологій, що залучають все більше і більше користувачів, які в процесі роботи обмінюються інформацією за допомогою систем електронного зв'язку, виникає необхідність розвитку засобів захисту інформації. Вирішити задачу захисту інформації можна шляхом використання криптографічних алгоритмів [1].

Розрізняють два типи криптографічних алгоритмів: симетричні і асиметричні. В першому випадку обидва абоненти, що беруть участь в процесі передачі інформації, використовують однаковий ключ, а в другому — різні, "секретний" і "відкритий".

В останні роки інтенсивно розвивається криптографія еліптичних кривих (ЕК), де основною криптографічною операцією є пошук кратних точок еліптичної кривої, тобто множення точки еліптичної кривої на скаляр на основі операції додавання цих точок [2]. Особливий інтерес до криптографії еліптичних кривих обумовлений такими перевагами – швидкодія та невелика довжина ключа.

У сучасних криптосистемах на основі еліптичних кривих бінарної розмірності в діапазоні від 150 до 350 забезпечується рівень криптографічної стійкості, який потрібно використовувати у відомих криптографічних системах бінарної розмірності від 600 до 1400 і більше.

У приведеній нижче табл. 1 порівнюються наближені розміри параметрів еліптичних систем і криптосистеми RSA, що забезпечують однакову стійкість шифру [1]. Ці дані отримані на основі сучасних методів розв'язання задачі дискретного логарифмування еліптичної кривої (Elliptic Curve Discrete Logarithm Problem – ECDLP) та факторизації (пошуку дільників) для великих цілих чисел.

Таблиця 1 – Порівняння стійкості основних криптографічних алгоритмів.

Система на основі еліптичної кривої (базова точка P)	RSA (довжина модуля n)
1024 біт	3084 біт
3250 біт	9750 біт
15500 біт	46500 біт

Як показує аналіз таблиці, використання еліптичних кривих дозволяє будувати стійкі системи з ключами значно менших розмірів у порівнянні з традиційними асиметричними криптоалгоритмами. Такі системи потребують меншого обсягу обчислювальних ресурсів, тому зручні для використання у смарт-картках та портативних телефонах.

На сьогодні еліптичні криві застосовують для реалізації різноманітних класів криптосистем, зокрема їх можна використовувати для побудови симетричних, асиметричних систем та систем електронного цифрового підпису (ЕЦП). На рис. 1 зображено класифікацію сучасних методів криптографії, що базуються на застосуванні еліптичних кривих. Аналіз показує, що математичний апарат еліптичних кривих можна застосовувати [1], [2], [6]:

1) в асиметричних криптосистемах;
2) в симетричних криптосистемах;
3) для реалізації електронного цифрового підпису;
4) для електронних платежів;
5) як генератори псевдовипадкових послідовностей.

Слід зауважити, що в літературі показано лише теоретичну можливість побудови симетричних криптосистем, стосовно ж практичної реалізації необхідно відмітити, що продуктивність таких систем є нижчою в порівнянні з традиційними.

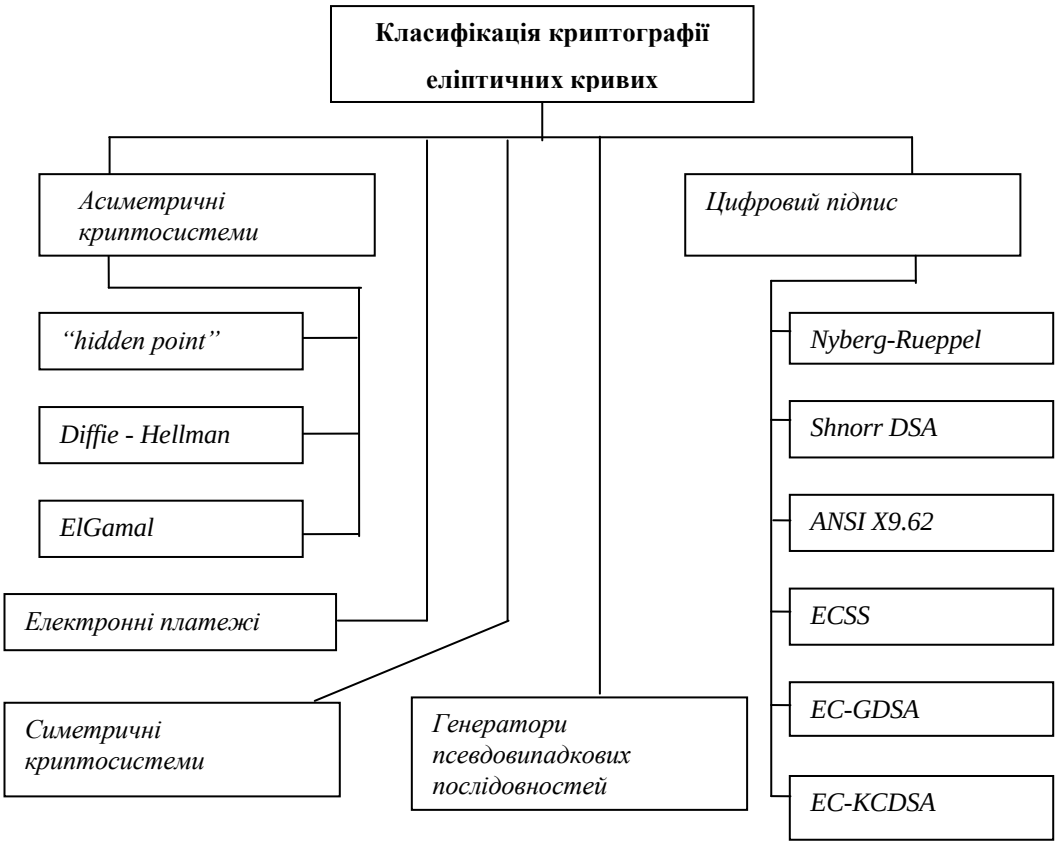

Рисунок 1 – Класифікація застосування еліптичних кривих для задач захисту інформації

II Проблеми застосування еліптичних кривих

Незважаючи на вагомі переваги існують і певні проблеми та труднощі застосування ЕК. Зокрема, виділяють такі класи задач:

1) генерування параметрів еліптичної кривої;
2) обчислення точок еліптичної кривої;
3) проблема дискретного логарифма.

В даній статті авторами розглядається проблема генерування параметрів ЕК.

Задачею генерування параметрів еліптичної кривої виду $y^2 = x^3 + ax + b(\mathrm{mod}p)$, де $a,b \in F_p^2$, $(x,y) \in F_p^2$, над простим полем GF(p) є знаходження таких параметрів:

a) просте число p – модуль перетворення груп точок еліптичної кривої;
b) просте число q, яке визначає порядок циклічної підгрупи групи точок еліптичної кривої ЕК [2];
c) коефіцієнти $a,b \in F_p^2$, що задають еліптичну криву ЕК.

Просте число p має задовольняти нерівність $p > 2^{255}$. Верхня границя значення числа визначається конкретною реалізацією криптосистеми. Для створення цифрового підпису довжиною 512 біт, як це було для стандарту ГОСТ 34.310-95, число p має задовольняти нерівність $p < 2^{256}$. В подальшому вважаємо, що число p лежить у межах $2^{255} < p < 2^{256}$.

Для генерації простого числа можна використовувати:

- процедуру генерації числа q в стандарті ГОСТ 34.310-95;
- генерацію випадкового простого числа довжиною 256 біт;
- генерацію сильного простого числа.

В стандарті X9.62-1998 пропонується 3 способи отримання параметрів еліптичної кривої [5]. Перший спосіб полягає у використанні кривих, заданих у стандарті X9.62-1998. Серед них тільки одна еліптична крива задовольняє потрібному простому числу. Другий спосіб полягає у випадковому виборі еліптичної кривої і перевірці її параметрів. Третій спосіб полягає в виборі потрібних параметрів і побудові кривої за цими параметрами.

Незважаючи на існуючі підходи до вирішення задачі генерування параметрів ЕК існують певні проблеми стосовно продуктивності генерування потрібного числа кривих за певний період часу. Тому актуальною залишається розробка нових методів, що дозволяють ефективно вирішити цю задачу.

IV Використання еволютивного підходу до задач генерування параметрів ЕК

Якщо на деякій множині задана складна (цільова) функція від кількох змінних, то еволютивний алгоритм – це алгоритм, який дозволяє за оптимальний час знаходити максимально наближене значення [4]. Таким чином еволютивний підхід може бути ефективно застосований для знаходження оптимальних (або квазі-оптимальних) рішень в задачах з обмеженням на часовий ресурс.

Для реалізації еволютивного підходу до вирішення задачі генерування параметрів еліптичної кривої авторами взято за основу алгоритм A.12.4. стандарту IEEE P1363. На основі цього алгоритму авторами розроблено алгоритм генерування параметрів еліптичної кривої з використанням еволютивного підходу. Схему запропонованого алгоритму зображено на рис. 1.

Ключовим моментом при розробці еволютивних алгоритмів є визначення критерію (цільової функції), на основі якого здійснюється відбір нових об'єктів. Авторами розроблено такий критерій на основі наведеного в стандарті співвідношення оцінки гладкості кривої :

$$f = c \cdot b^2(\mathrm{mod}p) - a^3(\mathrm{mod}p), \qquad (1)$$

де $a,b \in GF(p)$.

Робота розробленого алгоритму схожа з роботою типових генетичних алгоритмів і полягає в наступному. Спочатку в "Ініціалізації популяції" генеруються випадковим чином об'єкти з параметрами еліптичної кривої a,b. На наступному етапі здійснюється їх сортування в порядку зростання значення f. З першого етапу вибираються 1024 найкращі, тобто абсолютне значення критерію f (див. (1)) є найменшим, і заносяться в породжувальний масив. Далі здійснюється ітеративна процедура модифікації об'єктів P_i з породжувального масиву шляхом застосування операції мутації, причому в операторі мутації враховано напрям зміни коефіцієнтів a, b. Це дозволило суттєво підвищити ефективність роботи алгоритму. Далі обчислюється критерій f для отриманого шляхом мутації нового об'єкта. Якщо отримане абсолютне значення менше за попереднє, то новий об'єкт записується на місце попереднього (предка). В кінці алгоритму здійснюється перевірка на невиродженість отриманої еліптичної кривої.

На основі запропонованого алгоритму розроблено програмний засіб, який дозволяє отримати пари коефіцієнтів a, b, придатні для побудови стійких криптосистем на основі еліптичних кривих. Результати роботи програми наведено у табл. 2 і 3. Загалом було отримано більше 600 пар, проте після додаткової перевірки на невиродженість залишилось 208. В табл. 2 наведено коефіцієнти c_i, для яких згідно з алгоритмом розраховувалися коефіцієнти a, b.

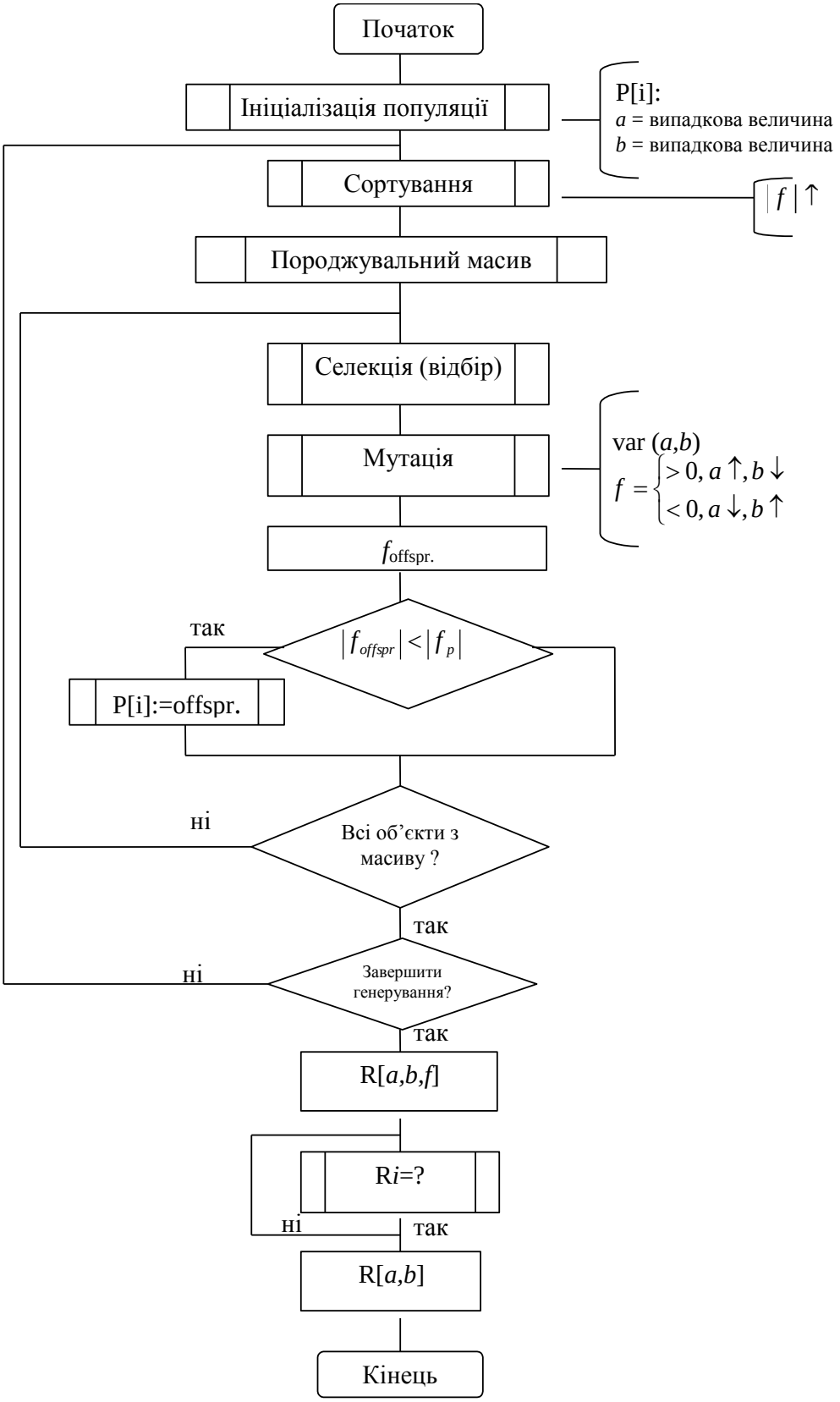

Рисунок 2 – Схема алгоритму генерування параметрів еліптичної кривої

Таблиця 2 – Коефіцієнти c_i.

Коефіцієнт c_i	Значення коефіцієнта
c_1	5179999668239675894400497456855545988819789197921163734568600903414731996719O
c_2	14186545527804375329915594346183841971258756371427817362289709707294098520 26
c_3	340029504799119145462029677206692577027644436517188412810134843965965744197 60
c_4	367171650888157766423778390433037732858905606854339925429282583561340337568 28
c_5	263594424922334526813969277922276547146511145874562904541092263506799693013 2
c_6	384505741217494040906279990521877869013955210103454062684854452154003290929 98

У табл. 3 наведено кількість згенерованих пар коефіцієнтів ЕК при певних коефіцієнтах c_i. Також в таблиці показано кількість пар коефіцієнтів a, b однакової та різної розмірності.

Для підвищення ефективності розробленого програмного засобу проводяться роботи щодо реалізації розподілених обчислень на кластері з 5–10 машин, об'єднаних в мережу. Це дасть змогу зменшити часовий ресурс та збільшити загальну кількість пар коефіцієнтів, що генеруються.

Таблиця 3 – Кількості згенерованих пар (a, b).

Коефіцієнт c	Загальна кількість пар	Кількість пар приблизно рівної розмірності $\lg a \approx \lg b$	Кількість пар різної розмірності $\lg a \neq \lg b$
c_1	4	1	3
c_2	18	9	9
c_3	16	5	11
c_4	20	7	13
c_5	125	63	62
c_6	25	16	9
Всього	208	101	107

V Висновки

Запропоновано алгоритм генерування параметрів еліптичної кривої для цифрового підпису, що дозволяє ефективно визначати коефіцієнти еліптичної кривої. Розроблений метод базується на еволютивному підході, що значно спрощує застосування запропонованого алгоритму на практиці. Наведено результати роботи програми, розробленої на основі даного методу, які підтверджують ефективність методу. Отже, доцільно використовувати розроблений метод в криптосистемах, що базуються на еліптичних кривих для захисту інформації на практиці.

Література: ***1.*** *Матеріали науково-практичного семінару „ДСТУ 4145-2002. Інформаційні технології. Криптографічний захист інформації. Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка". Київ – 2003.* ***2.*** *Elliptic Curve Cryptography. Certicom Research, 1999. Working Draft.* ***3.*** *IEEE P1363 / D8(Draft Version 8). Standard Specifications for Public Key Cryptography.* ***4.*** *Исаев С. Генетические алгоритмы – эволюционные методы поиска, http://ai-online.fromru.com/documents-genetic_algorithms.html.* ***5.*** *X9.62-1998.* ***6.*** *Сравнительный анализ ЦП в группах точек эллиптических кривых / И. Д. Горбенко, С. И. Збитнев, А. А. Поляков // Радиотехника: Всеукр. Межвер. Научн.-техн. Сб. 2002. Вып. 126. С. 71–84.* ***7.*** *Генерація параметрів та ключів для цифрового підпису на еліптичних кривих для скінченого простого поля / І. Д. Горбенко, О. Г. Качко, П. В. Колесніков // Радіотехніка: Всеукр. міжвід. наук.-техн. зб. 2002., вип. 126. с. 193–198.*